A/74/48037

Advance Unedited Version

Distr.: General
11 October 2019

Original: English

Seventy-fourth session
Item 72(b) of the provisional agenda*
Promotion and protection of human rights: Human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms

Report of the Special rapporteur on extreme poverty and human rights**

Note by the Secretary-General

The Secretary-General has the honour to transmit to the General Assembly the report of the Special Rapporteur on extreme poverty and human rights, Philip Alston, submitted in accordance with Human Rights Council resolution 35/19.

Summary

The digital welfare state is either already a reality or is emerging in many countries across the globe. In these states, systems of social protection and assistance are increasingly driven by digital data and technologies that are used to automate, predict, identify, surveil, detect, target and punish. This report acknowledges the irresistible attractions for governments to move in this direction, but warns that there is a grave risk of stumbling zombie-like into a digital welfare dystopia. It argues that Big Tech operates in an almost human rights free-zone, and that this is especially problematic when the private sector is taking a leading role in designing, constructing, and even operating significant parts of the digital welfare state. The report recommends that instead of obsessing about fraud, cost savings, sanctions, and market-driven definitions of efficiency, the starting point should be on how welfare budgets could be transformed through technology to ensure a higher standard of living for the vulnerable and disadvantaged.

* A/74/50.

** The present report was submitted after the deadline in order to reflect the most recent developments.

Contents

		Page
I.	Introduction	3
II.	Uses of digital technologies in the welfare state	5
	A. Identity verification	5
	B. Eligibility assessment	7
	C. Welfare benefit calculation and payments	8
	D. Fraud prevention and detection	8
	E. Risk scoring and need classification	9
	F. Communication between welfare authorities and beneficiaries	9
III.	Making digital technologies work for social protection	10
	A. Taking human rights seriously and regulating accordingly	11
	B. Ensuring legality and transparency	12
	C. Promoting digital equality	13
	D. Protecting economic and social rights in the digital welfare state	14
	E. Protecting civil and political rights in the digital welfare state	15
	F. Resisting the inevitability of a digital only future	17
	G. The role of the private sector	18
	H. Accountability mechanisms	18
IV.	Conclusions	19

I. Introduction[1]

1. The era of digital governance is upon us. In high and middle income countries, electronic voting, technology-driven surveillance and control including through facial recognition programs, algorithm-based predictive policing, the digitization of justice and immigration systems, online submission of tax returns and payments, and many other forms of electronic interactions between citizens and different levels of government are becoming the norm. And in lower income countries, national systems of biometric identification are laying the foundations for comparable developments, especially in systems to provide social protection, or 'welfare', to use a shorthand term.[2]

2. Invariably, improved welfare provision, along with enhanced security, is one of the principal goals invoked to justify the deep societal transformations and vast expenditures that are involved in moving the entire population of a country not just on to a national unique biometric identity card system but on to linked centralized systems providing a wide array of government services and the provision of goods ranging from food and education to health care and special services for the ageing or those with disabilities.

3. The result is the emergence of the 'digital welfare state' in many countries across the globe.[3] In these states, systems of social protection and assistance are increasingly driven by digital data and technologies that are used to automate, predict, identify, surveil, detect, target and punish. The process is commonly referred to as 'digital transformation', but this somewhat neutral term should not be permitted to conceal the revolutionary, politically-driven, character of many such innovations. Commentators have predicted "a future in which government agencies could effectively make law by robot",[4] and it is clear that new forms of governance are emerging which rely significantly on the processing of vast quantities of digital data from all available sources, use predictive analytics to foresee risk, automate decision-making, and remove discretion from human decision-makers. In such a world, citizens become ever more visible to their governments, but not the other way around.[5]

4. Welfare is an attractive entry point not just because it takes up a major share of the national budget or affects such a large proportion of the population but because digitization can be presented as an essentially benign initiative. Thus, for example, the United Kingdom's digital strategy proclaims that it will "transform the relationship between citizens and the state", thus "putting more power in the hands

[1] This report has been prepared in close collaboration with Christiaan van Veen, Director of the Digital Welfare States and Human Rights Project, at New York University School of Law.

[2] While welfare is often used as a pejorative term, it is used in a positive sense in this report and is synonymous with the goal of social protection as reflected in the ILO's Social Protection Floor initiative and comparable approaches. See generally David Garland, *The Welfare State: A Very Short Introduction* (2016).

[3] Philip Alston and Christiaan van Veen, 'How Britain's welfare state has been taken over by shadowy tech consultants', *The Guardian*, 27 June 2019.

[4] Cary Coglianese and David Lehr, 'Regulating by Robot: Administrative Decision Making in the Machine-Learning Era', *Georgetown Law Journal* (Vol. 105, 2017), p. 1147.

[5] Compare Foucault's description of Panoptic systems where those put under surveillance are "seen, without ever seeing". Michel Foucault, *Discipline and Punish: The Birth of the Prison* (1977), p. 202.

of citizens and being more responsive to their needs." In India, the core values of the Unique Identification Authority of India include: facilitating good governance, integrity, inclusive nation building, a collaborative approach, excellence in services, and transparency and openness.

5. In other words, the embrace of the digital welfare state is presented as an altruistic and noble enterprise designed to ensure that citizens benefit from new technologies, experience more efficient government, and enjoy higher levels of well-being. Often, however, the digitization of welfare systems has been accompanied by deep reductions in the overall welfare budget, a narrowing of the beneficiary pool, the elimination of some services, the introduction of demanding and intrusive forms of conditionality, the pursuit of behavioural modification goals, the imposition of stronger sanctions regimes, and a complete reversal of the traditional notion that the state should be accountable to the individual.

6. These other outcomes are promoted in the name of efficiency, targeting, incentivizing work, rooting out fraud, strengthening responsibility, encouraging individual autonomy, and responding to the imperatives of fiscal consolidation. Through the invocation of what are often ideologically-charged terms, neoliberal economic policies are seamlessly blended into what are presented as cutting edge welfare reforms, which in turn are often facilitated, justified, and shielded by new digital technologies. Although the latter are presented as being 'scientific' and neutral, they can reflect values and assumptions that are far removed from, and may be antithetical to, the principles of human rights. In addition, because of the relative deprivation and powerlessness of many welfare recipients, conditions, demands and forms of intrusiveness are imposed that would never have been accepted if they had instead been piloted in programs applicable to better-off members of the community.

7. Despite the enormous stakes involved not just for millions of individuals but for societies as a whole, these issues have, with a few notable exceptions,[6] garnered remarkably little attention. The mainstream tech community has been guided by official pre-occupations with efficiency, budget-savings, and fraud detection. The welfare community has tended to see the technological dimensions as separate from the policy developments, rather than as being integrally linked. And those in the human rights community concerned with technology have understandably been focused instead on concerns such as the emergence of the surveillance state, the potentially fatal undermining of privacy, the highly discriminatory impact of many algorithms, and the consequences of the emerging regime of surveillance capitalism.

8. But the threat of a digital dystopia is especially significant in relation to the emerging digital welfare state. This report aims to redress the neglect of these issues to date by providing a systematic account of the ways in which digital technologies are used in the welfare state and of their implications for human rights. It concludes by calling for the regulation of digital technologies, including artificial intelligence, to ensure compliance with human rights, and for a rethinking of the positive ways in which the digital welfare state could

[6] For pioneering work on the impact of digital technologies on the American welfare state, especially on the poorest individuals in the system, see Virginia Eubanks, *Automating Inequality (*2018). See also Cathy O'Neil, *Weapons of Math Destruction* (2016) and Khiara Bridges, *The Poverty of Privacy Rights* (2017).

be a force for the achievement of vastly improved systems of social protection.

9. The report builds in part on country reports by the Special Rapporteur on visits to the United States in 2017 and the United Kingdom in 2018 which drew attention to the increasing use of digital technologies in social protection systems. In preparing the report, the Special Rapporteur consulted with representatives of various digital rights groups, leading scholars, and other stakeholders, first in a meeting hosted by the Digital Freedom Fund in Berlin in February 2019, and then at another sponsored by the Center for Information Technology Policy at Princeton University in April 2019.[7] In addition, a formal call for contributions resulted in some 60 submissions from 34 countries,[8] including 22 governments, as well as international and national civil society organizations, National Human Rights Institutions, academics, and individuals. While it is impossible to do justice to these rich and detailed submissions in such a necessarily brief report, the Special Rapporteur has made them electronically available[9] and will continue analyzing them in the context of ongoing work on the digital welfare state.[10]

II. Uses of digital technologies in the welfare state

10. From the many submissions received, and on the basis of various case studies addressed in the literature, it is possible to distinguish various ways, and different stages in the welfare context, in which digital innovation has been most prominently used.

A. Identity verification

11. Establishing every person's legal identity, including through birth registration, by the year 2030 is the aim of Sustainable Development Goal (SDG) 16.9. A verifiable identity is essential for applying for benefits, establishing entitlement, receiving benefits, and appealing against denial. For the Government or other provider, it avoids duplication and fraud, it facilitates accurate targeting, and it enhances efficiency. Traditionally, paper and/or plastic documents have been used in forms such as birth certificates, identity cards and passports. These systems function reasonably well in most of the Global North, although 21 million adults in the United States do not have government-issued photo ID.[11] In the Global South, 502 million people in sub-Saharan Africa and 357 million in South Asia lack official

[7] https://www.princeton.edu/news/2019/04/18/panelists-tell-un-expert-artificial-intelligence-offers-promise-and-peril-social.

[8] From: Argentina, Australia, Austria, Azerbaijan, Brazil, Chile, Croatia, Egypt, El Salvador, Estonia, Germany, Greece, Guatemala, India, Italy, Ireland, Kazakhstan, Lebanon, Mexico, Nicaragua, Nigeria, Netherlands, New Zealand, Oman, Pakistan, Philippines, Poland, Qatar, Russian Federation, Senegal, South Africa, Switzerland, United Kingdom, and the United States.

[9] https://www.ohchr.org/EN/Issues/Poverty/Pages/SubmissionsGADigitalTechnology.aspx.

[10] https://chrgj.org/people/christiaan-van-veen/.

[11] https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/PrivacyInternational.pdf

identification.[12] In Liberia, for example, birth registration stands at only 5 per cent and national identity cards were not introduced until 2015.[13]

12. In response, the World Bank, regional development organizations and bilateral donors have launched new programs to promote access to identity documents. In particular, the World Bank's 'ID4D' (Identification for Development)[14] campaign has focused heavily on promoting digital technologies as the key solution. This is explicitly stated in the 'Principles on Identification for Sustainable Development', which have been widely endorsed, including by MasterCard.[15]

13. The Principles acknowledge that there are both pros and cons involved. On the positive side, it is claimed that digital technology can "create huge savings for citizens, governments, and businesses by reducing transaction costs, increasing efficiency, and driving innovation in service delivery, particularly to the poorest and most disadvantaged groups in society".[16] Digital identity systems can also "improve governance, boost financial inclusion, reduce gender inequalities by empowering women and girls, and increase access to health services and social safety nets for the poor".[17]

14. But in addition to this impressive and by now familiar sales pitch, the Principles, and similar documents,[18] also recognize possible downsides ranging from political backlash to privacy and (cyber)security concerns. Solutions for dealing with those risks are often either technological or take the form of soft law norms. Thus a comparable United States Agency for International Development (USAID) document calls for "open source solutions" and developing good "practices for data privacy" to resolve the relevant problems. While the World Bank Principles refer to isolated human rights principles such as Article 7 of the Convention on the Rights of the Child, they rely primarily on the need to create an interoperable system using open standards, and protecting 'privacy through system design'.

15. The world's largest biometric identification system is Aadhaar in India, which is a 12-digit unique identifying number issued to Indian residents. It contains both demographic and biometric information, including an iris scan, a photograph and fingerprints. It is used to verify the identity of recipients of benefits and subsidies and is now mandatory to access those social rights.[19] It was first introduced in 2009

12 USAID, 'Identity in a Digital Age' (2017), p. 8.

13 Bronwen Manby, *Citizenship in Africa* (2018), p. 3.

14 https://id4d.worldbank.org/

15 World Bank and Center for Global Development, 'Principles on Identification for Sustainable Development: Toward the Digital Age', February 2017, at http://documents.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identification-for-sustainable-development-toward-the-digital-age.pdf

16 World Bank and Center for Global Development, 'Principles on Identification for Sustainable Development: Toward the Digital Age', February 2017, p. 5, available from: http://documents.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identification-for-sustainable-development-toward-the-digital-age.pdf;

17 Id.

18 USAID, 'Identity in a Digital Age' (2017); McKinsey, 'Digital Identification: A Key to Inclusive Growth', January 2019, at https://www.mckinsey.com/~/media/mckinsey/featured%20insights/innovation/the%20value%20of%20digital%20id%20for%20the%20global%20economy%20and%20society/digital-id-a-key-to-inclusive-growth-january%202019.ashx

19 See, e.g., Centre for Communication Governance at National Law University Delhi, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/NationalLa

and now covers more than 1.2 billion people,[20] and has been enthusiastically endorsed by the international development community.[21] The World Bank has praised it for "overcoming complex information problems, [thereby helping] willing governments to promote the inclusion of disadvantaged groups",[22] and has enthusiastically encouraged other governments to learn from the experience,[23] and over 20 countries are reported to have expressed an interest in emulating Aadhaar.[24]

16. It nevertheless remains controversial domestically. Critics have reportedly been harassed and surveilled for their opposition,[25] and the scheme has been criticized for unnecessarily collecting biometric information, for severe shortcomings in legislative oversight, function creep, facilitating surveillance and other intrusions on the right to privacy, exacerbating cybersecurity issues, and creating barriers to accessing a range of social rights.[26]

17. In 2018 India's Supreme Court, in a 1448-page landmark ruling, upheld Aadhar's constitutionality, albeit with some caveats. The court appeared to view the use of biometric identification technology in the context of providing welfare benefits as being legitimate, proportional and even inevitable. In a welfare state, Aadhaar's aim of ensuring that benefits reach the intended beneficiary was "naturally a legitimate State aim".[27] In balancing the rights to social security and privacy, the court held that registering biometric data represented a 'minimal' inroad into privacy rights,[28] and went so far as to characterize Aadhaar as "a vital tool of ensuring good governance in a social welfare state".[29] But the Supreme Court's ruling has apparently not put an end to the controversy surrounding the scheme.[30]

18. In 2019 Kenya required all of its citizens, including those living abroad, and all foreign nationals and refugees in the country, above the age of 6, to obtain a national ID in order to access government services, including welfare benefits.[31] This involved providing biometric data including fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves and DNA in digital form. In response to a case claiming that this Huduma Namba program violated the rights to

wUniversityDelhi.pdf.

20 https://economictimes.indiatimes.com/news/politics-and-nation/national-population-register-to-include-aadhaar-details/articleshow/70528850.cms?from=mdr.

21 Jeanette Rodrigues, 'India ID Program Wins World Bank Praise Despite 'Big Brother' Fears', 15 March 2017, available from: https://www.bloomberg.com/news/articles/2017-03-15/india-id-program-wins-world-bank-praise-amid-big-brother-fears.

22 World Bank, *World Development Report 2016*, p. 2.

23 https://www.livemint.com/Politics/UEQ9o8Eo8RiaAaNNMyLbEK/Aadhaar-goes-global-finds-takers-in-Russia-and-Africa.html.

24 https://factordaily.com/aadhaar-india-stack-export/.

25 https://www.reuters.com/article/us-india-aadhaar-breach/critics-of-indias-id-card-project-say-they-have-been-harassed-put-under-surveillance-idUSKBN1FX0H0

26 Submission to the Special Rapporteur by the National Law University, Delhi.

27 Supreme Court of India, Writ Petition (Civil) No. 494 of 2012, p. 341.

28 Id., p. 377.

29 Id., p. 553.

30 https://www.nytimes.com/2018/09/26/technology/india-id-aadhaar-supreme-court.html.

31 Amnesty International, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/AmnestyInternational.pdf.

privacy, equality, non-discrimination and public participation, the High Court issued an interim order allowing the registration process to continue, but on a voluntary basis and on the basis that the disbursement of government services and benefits could not be made conditional on participation. Subsequently, registration has proceeded apace, some two-thirds of the population has been registered,[32] and the Government is reportedly threatening to exclude unregistered individuals from access to benefits or the right to vote.[33]

19. In South Africa, the South African Social Security Agency (SASSA), distributes non-contributory and means-tested social grants to around one-third of the population, including for example grants for child support, for pensioners, and for persons with disabilities.[34] In 2012, SASSA contracted with the company Cash Paymaster Services (CPS), a subsidiary of Net1, to deliver the grants.[35] CPS registered beneficiaries by collecting their biometric information (finger prints and, originally, voice recordings) and beneficiaries were issued MasterCard debit cards with biometric functionality and a linked bank account by Net1 and Grindrod Bank in association with SASSA.[36] After much controversy surrounding the tender to CPS, the fees charged by CPS, deductions made to social grants on these accounts as well as privacy concerns surrounding the processing of card holder data, SASSA changed providers in 2018 by entering into a partnership with the South African Post Office (SAPO). SASSA and SAPO will provide new biometric cards. The change from CPS to SAPO has been complex and has led to questions about effective access to social grants by beneficiaries in South Africa.[37]

20. Many other examples could be given of countries using or exploring digital identity systems, including Argentina,[38] Bangladesh,[39] Chile,[40] Ireland, Jamaica,[41] Malaysia,[42] the Philippines,[43] and the United States.[44]

32 Id.

33 https://www.standardmedia.co.ke/article/2001334286/you-ll-miss-vital-services-without-huduma-namba.

34 https://www.dfa.co.za/news/budget2019-social-grants-to-increase-19404725.

35 Black Sash, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/BlackSash.pdf.

36 https://newsroom.mastercard.com/press-releases/more-than-2-5-million-mastercard-debit-cards-issued-to-social-welfare-beneficiaries-in-south-africa/.

37 https://citizen.co.za/business/1944057/post-office-set-to-take-over-cash-payments-from-cps/.

38 Submission to the Special Rapporteur by the Government of Argentina.

39 https://privacyinternational.org/examples/2878/bangladesh-biometrics-needed-access-welfare-payment.

40 In Chile, facial recognition technology is used to deliver school meals: See https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/PrivacyInternational.pdf.

41 https://opm.gov.jm/portfolios/national-identification-system/.

42 https://www.opengovasia.com/malaysias-digital-id-project-to-be-finalised-by-2019/.

43 https://psa.gov.ph/philsys.

44 See for example the use of digital technologies in the CalWORKs program in California, the United States, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/HumanRightsWatch.pdf.

B. Eligibility assessment

21. Automated programs are increasingly used to assess eligibility in many countries. An especially instructive case was the automation of eligibility decisions in Ontario in 2014 through the Social Assistance Management System (SAMS) which relied on Cúram, a customizable off-the-shelf IBM software package, also used in welfare programs in Canada, the United States, Germany, Australia and New Zealand.[45]

22. In 2015 the Ontario Auditor-General reported on 1,132 cases of errors with eligibility determinations and payment amounts under SAMS involving about $140 million. The total expenditure on SAMS by late 2015 was $290 million.[46] The new system reportedly led caseworkers to resort to subterfuges to ensure that beneficiaries were fairly treated, made decisions very difficult to understand, and created significant additional work for staff.[47]

C. Welfare benefit calculation and payments

23. The calculation and payment of benefits is increasingly done through digital technologies without the involvement of caseworkers and other human decision-makers. While such systems offer many potential advantages, the Special Rapporteur also received information about prominent examples of system errors or failures that generated major problems for large numbers of beneficiaries. These included the 'Robodebt' fiasco in Australia,[48] the Real Time Information system in the United Kingdom,[49] and the SAMS system in Canada.

24. Electronic payment cards or debit cards are also increasingly being issued to welfare recipients. Information provided to the Special Rapporteur in relation to such programs in New Zealand, Australia and South Africa reveal very similar problems. First, beneficiaries often face difficulties accessing and fully utilizing their right to social security.[50] Second, when such cards are clearly recognizable as welfare-related, users have expressed feelings of disempowerment, embarrassment and shame,[51] a problem exacerbated when the users come from communities long accustomed to exclusion.[52] Third, electronic cards enable monitoring and surveillance of behavioral data by welfare

45 Submission to the Special Rapporteur by Human Rights Watch, available from: https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/HumanRightsWatch.pdf.

46 *2015 Annual Report of the Office of the Auditor General of Ontario*, p. 475.

47 Jennifer Raso, 'Displacement as Regulation: New Regulatory Technologies and Front Line Decision Making in Ontario Works', *Canadian Journal of Law and Society,* Vol. 32, (2017) 75.

48 Terry Carney, 'The New Digital Future for Welfare: Debts Without Legal Proofs or Moral Authority?', *UNSW Law Journal Forum* (March, 2018) p. 1; Report by the Acting Commonwealth Ombudsman, Richard Glenn, 'Centrelink's automated debt raising and recovery system', April 2017, p. 7-8; Submission to the Special Rapporteur by Monash University.

49 Statement on Visit to the United Kingdom, 16 November 2018, at: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23881&LangID=E.

50 https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/GriffithUniversity.docx.

51 https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/NicoleNaujokas.docx.

authorities and private actors, thus raising important human rights concerns.[53]

25. Fourth, the outsourcing of the issuance and administration of electronic cards to private companies has led to problems such as users being encouraged to pay for commercial financial products and the imposition of user fees.[54] More generally the ethos surrounding such cards has often reflected stereotypes such as the financial untrustworthiness and irrationality of those living in poverty.

D. Fraud prevention and detection

26. Fraud and error in welfare systems can potentially involve very large sums of money and have long been a major concern for governments. It is thus unsurprising that many of the digital welfare systems that have been introduced have been designed with a particular emphasis on the capacity to match data from different sources in order to expose deception and irregularities on the part of welfare applicants. Nevertheless, evidence from country missions undertaken by the Special Rapporteur,[55] along with other cases examined,[56] suggests that the magnitude of these problems is frequently overstated and that there is sometimes a wholly disproportionate focus on this particular dimension of the complex welfare equation. Images of supposedly wholly undeserving individuals receiving large government welfare payments, such as Ronald Reagan's 'welfare queen' trope, have long been used by conservative politicians to discredit the very concept of social protection. The risk is that the digital welfare state provides endless possibilities for taking surveillance and intrusion to new and deeply problematic heights.

E. Risk scoring and need classification

27. Risk calculation is inevitably at the heart of the design of welfare systems and digital technologies can achieve very high levels of sophistication in this regard. In addition to fraud detection and prevention, child protection has been a major focus in this area, as illustrated by examples from countries as diverse as the United States,[57] New Zealand,[58] the United Kingdom,[59] and Denmark.[60] Governments have also applied these techniques to determine whether

52 https://www.theguardian.com/australia-news/2017/jan/09/ration-days-again-cashless-welfare-card-ignites-shame.

53 https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/UniversityAuckland.docx.

54 http://theconversation.com/the-real-risks-behind-south-africas-social-grant-payment-crisis-73224

55 Statement on Visit to the United Kingdom, by Professor Philip Alston, United Nations Special .Rapporteur on extreme poverty and human rights, 16 November 2018, available from: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23881&LangID=E.

56 See the SyRI case from the Netherlands, n86 below.

57 Virginia Eubanks, *Automating Inequality* (2018); Alexandra Chouldechova et. al., 'A case study of algorithm-assisted decision making in child maltreatment hotline screening decisions', *Proceedings of Machine Learning Research* 81:1–15, 2018; https://www.nytimes.com/2018/01/02/magazine/can-an-algorithm-tell-when-kids-are-in-danger.html.

58 Philip Gillingham, 'Predictive Risk Modelling to Prevent Child Maltreatment: Insights and Implications from Aotearoa/New Zealand', *Journal of Public Child Welfare* (Vol. 11, 2017), p. 150.

unemployment assistance will be provided and at what level. A prominent such scheme in Poland was held unconstitutional,[61] but an algorithm-based system in Austria continues to categorize unemployed jobseekers to determine the support they will receive from government jobcenters.[62]

28. Many other areas of the welfare state will also be affected by new technologies used to score risks and classify needs.[63] While such approaches offer many advantages, it is also important to take account of the problems that can arise. First there are many issues raised by determining an individual's rights on the basis of predictions derived from the behavior of a general population group.[64] Second, the functioning of the technologies and how they arrive at a certain score or classification is often secret, thus making it difficult to hold governments and private actors to account for potential rights violations.[65] Third, risk-scoring and need categorization can reinforce or exacerbate existing inequalities and discrimination.[66]

F. Communication between welfare authorities and beneficiaries

29. Communications that previously took place in person, by phone or by letter are increasingly being replaced by online applications and interactions. Various submissions to the Special Rapporteur cited problems with the Universal Credit system in the United Kingdom, including difficulties linked to a lack of internet access and/or digital skills,[67] and the extent to which online portals can create confusion and obfuscate legal decisions, thereby undermining the right of claimants to

59 https://www.theguardian.com/society/2018/sep/16/councils-use-377000-peoples-data-in-efforts-to-predict-child-abuse; https://www.communitycare.co.uk/2019/06/14/county-becomes-latest-authority-trial-predictive-algorithms-childrens-social-work/.

60 https://foreignpolicy.com/2018/12/25/the-welfare-state-is-committing-suicide-by-artificial-intelligence/.

61 Polish Supreme Court, case K 53/16, 6 June 2018, http://trybunal.gov.pl/postepowanie-i-orzeczenia/komunikaty-prasowe/komunikaty-po/art/10168-zarzadzanie-pomoca-kierowana-do-osob-bezrobotnych.

62 EpicenterWorks, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/EpicenterWorks.pdf

63 See, for example, Data Justice Lab, 'Data Scores as Governance: Investigating uses of citizen scoring in public services', December 2018.

64 University of Queensland, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/University_of_Queensland.pdf; and Data Justice Lab, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/UniversityCardiff.pdf ("Household-level and individual-level data relies on a fundamental personalization of risk, attaching risk factors to individual characteristics and behaviour that can lead to individualized responses to social ills being privileged over collective and structural responses, such as issues of inequality, poverty or racism.").

65 London School of Economics and Political Science, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/LSE.pdf.

66 "But human bias is built in to the predictive risk model." https://www.wired.com/story/excerpt-from-automating-inequality/.

67 Scottish Council for Voluntary Organisations, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/ScottishCouncilVoluntaryOrganisations.pdf; and Citizens Advice Scotland, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/ChildPovertyActionsGroup_1.pdf.

understand and appeal decisions affecting their social rights.[68] Similar issues were also raised in relation to other countries including Australia,[69] and Greece.[70]

30. Another problem is the likelihood that once the entire process of applying and maintaining benefits is moved online, the situation invites further digital innovation. In 2018 Sweden was forced to reverse a complex digital system used by the Employment Service to communicate with jobseekers because of problems that led to as many as 15% of the system's decisions probably being incorrect.[71]

31. Australia's Targeted Compliance Framework (TCF) requires job seekers to interact with a digital dashboard to report mandatory activities and to check their compliance status. Failure to meet a 'mutual obligation' can automatically, without the involvement of a human decision-maker, lead to suspension of payments or the imposition of financial penalties. Submissions have highlighted problems due to a lack of internet access and digital literacy, to the rigidity of an automated system which fails to take real-life situations into account.[72]

III. Making digital technologies work for social protection

32. Digital technologies, including artificial intelligence, have huge potential to promote the many benefits that are consistently cited by their proponents. They are already doing so for those who are economically secure and can afford to pay for the new services. They could also make an immense positive difference in improving the well-being of the less well-off members of society, but this will require deep changes in existing policies. The leading role in any such effort will have to be played by governments through appropriate fiscal policies and incentives, regulatory initiatives, and a genuine commitment to designing the digital welfare state not as a Trojan Horse for neoliberal hostility towards welfare and regulation but as a way to ensure a decent standard of living for everyone in society.

33. This report has sought to highlight problems that are specific to the ways in which the digital welfare state has been envisioned and implemented. But many of the changes required to avoid a digital dystopia will need to range more broadly. In addressing the General Assembly on 24 September 2019 the Prime Minister of the United Kingdom warned of the dangers of the digital age, singling out: (i) the risk of 'round-the-clock surveillance'; (ii) the perils of algorithmic

[68] Child Poverty Action Group, 'Computer Says No!', May 2019, available from: https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/ChildPovertyActionsGroup_2.pdf.

[69] Senate Community Affairs References Committee, Parliament of Australia, *Design, scope, cost-benefit analysis, contracts awarded and implementation associated with the Better Management of the Social Welfare System Initiative* (June, 2017), p. 60.

[70] Submission to the Special Rapporteur by the Government of Greece.

[71] AlgorithmWatch, 'Sweden: Rogue algorithm stops welfare payments for up to 70,000 unemployed', 19 February 2019.

[72] Human Rights Law Centre, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/HumanRightsLawCentre.pdf; and https://www.nssrn.org.au/social-security-rights-review/the-targeted-compliance-framework-implications-for-job-seekers/.

decision-making; (iii) the difficulty of appealing against computer-generated determinations; and (iv) the inability to plead extenuating circumstances when the decision-maker is an algorithm. He concluded rather ominously by suggesting that "[d]igital authoritarianism is … an emerging reality."[73]

34. His comments resonate strongly in the context of the digital welfare state, including in relation to the United Kingdom's Universal Credit system. There is no magic recipe for avoiding the pitfalls of which he warned, but the following steps could help to make the digital welfare state a force for enhancing rather than undermining human rights.

A. Taking human rights seriously and regulating accordingly

35. The United Kingdom Prime Minister concluded his speech by warning that "[u]nless we ensure that new technology reflects" human rights, the Universal Declaration of Human Rights "will mean nothing … ."[74] But the reality is that governments have certainly not regulated the tech industry as if human rights were at stake, and the technology sector remains virtually a human rights-free zone. The Big Tech companies and their governmental supporters have worked hard to keep it that way. Their approach can be summed up for present purposes in four propositions.

36. The first is that the ability to innovate requires freedom, especially from regulation. The Facebook founder's early call for the industry to "move fast and break things" epitomizes the importance attached to minimizing legal and governmental constraints. Yet this argument leads inexorably to a handful of powerful executives replacing governments and legislators in determining the directions in which societies will move and the values and assumptions which will drive those developments. The accumulation of vast amounts of capital in the hands of very small elites and the rapid growth in extreme inequality have gone hand in hand with the ascendency of this approach so far.[75]

37. The second proposition is that there are no universal values. In a recent book, the President of Microsoft asked rhetorically: "How can the world converge on a singular approach to ethics for computers when it cannot agree on philosophical issues for people?"[76] Even non-discrimination standards are sometimes presented as being too vague and contested to be useful in regulating AI.[77] But these arguments are self-serving and ill-informed. Governments worldwide have accepted universal human rights standards, including in the form of binding legal obligations. And over the past half century or more, these standards have been exhaustively developed and applied by courts, and a wide range of expert and community-based bodies. There remains plenty of

[73] https://www.gov.uk/government/speeches/pm-speech-to-the-un-general-assembly-24-september-2019.

[74] Id.

[75] See generally Shoshana Zuboff, *The Age of Surveillance Capitalism* (2019); and Emmanuel Saez and Gabriel Zucman, *The Triumph of Injustice: How the Rich Dodge Taxes and How to Make Them Pay* (2019).

[76] Brad Smith and Carol Ann Browne, *Tools and Weapons: The Promise and the Peril of the Digital Age* (2019), p. 207.

[77] *Public Scrutiny of Automated Decisions: Early Lessons and Emerging Methods, An Upturn and Omidyar Network Report* (2018), p. 25, and n. 115 at https://www.omidyar.com/sites/default/files/file_archive/Public%20Scrutiny%20of%20Automated%20Decisions.pdf.

room for philosophical disagreements, but there is no absence of agreement on core human values.

38. The third proposition is that governments are inherently slow and clumsy, and tend to respond to yesterday's challenges rather than tomorrow's. As the Republican minority leader of the United States House of Representatives recently argued, "the bureaucratic leviathan [does not have] what it takes to develop or enforce nimble responses to rapid change in the technology industry."[78] But while such claims might also be put forward by the proponents of unfettered discretion for the finance, aviation, defence, pharmaceutical, and other industries, it is solely in relation to Big Tech that governments have been prepared to abandon their regulatory responsibilities and acquiesce in a self-regulatory approach to such an extreme degree. There is no justification for such exceptionalism and no empirical evidence to support the claim that there is a fundamental incompatibility between innovation and regulation.

39. And the fourth proposition is that public accountability is unnecessary because the free market is the best regulator.[79] Leaving aside the powerful arguments that Big Tech is deeply anti-competitive and thus immune to many currents of the free market, the great scandals of recent years that have led to the so-called 'techlash' provide compelling evidence that public accountability is indispensable.

40. In response to growing calls for effective governmental regulation, the industry has gone into high gear in producing, influencing and embracing 'codes of ethics' and other non-binding standards purporting to 'regulate' digital technologies and their developers.[80] Most, but by no means all, of these codes contain a reference to human rights, but the substance of human rights law is invariably lacking. Instead the token reference to human rights serves only to enhance claims to legitimacy and universality. Meanwhile, the relevant discussions of ethics are based on almost entirely open-ended notions that are not necessarily grounded in legal or even philosophical arguments, and can be shaped to suit the needs of the industry. As a result, there are serious problems of conceptual incoherence, conflicts among norms are rarely acknowledged, meaningful input is rarely sought from stakeholders, and accountability mechanisms are absent.[81] Even industry-employed ethicists acknowledge that "[i]f ethics is simply absorbed within the logics of market fundamentalism, meritocracy, and technological solutionism, it is unlikely that the tech sector will be able to offer a meaningful response to the desire for a more just and values-driven tech ecosystem."[82] Against this background, it is unsurprising that there

78 Kevin McCarthy, 'Don't Count on Government to Protect Your Privacy', *New York Times*, 14 June 2019.

79 See generally Julie Cohen, 'Law for the Platform Economy', *51 U.C. Davis L. Rev. 133* (2017).

80 These include industry standards, civil society initiatives and public frameworks. To give a few examples: IBM, 'Everyday Ethics for Artificial Intelligence' (September 2018); Google, 'AI Principles' (2019); Microsoft, *The Future Computed* (2018); IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems; SIIA, 'Ethical Principles for Artificial Intelligence and Data Analytics' (2017); Asilomar AI Principles (2017); Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, 'Ethics Guidelines for Trustworthy AI' (April 2019).

81 Karen Yeung, Andrew Howes, and Ganna Pogrebna, 'AI Governance by Human Rights-Centred Design, Deliberation and Oversight: An End to Ethics Washing', forthcoming in M Dubber and F Pasquale (eds.), *The Oxford Handbook of AI Ethics* (2019), at https://ssrn.com/abstract=3435011, p. 22.

82 Jacob Metcalf, Emanuel Moss, and danah boyd [sic], 'Owning Ethics: Corporate Logics, Silicon Valley, and the Institutionalization of Ethics', 82

are few public or scholarly discussions of the *human rights* implications of digital welfare states.

41. The human rights community has thus far done a very poor job of persuading industry, government, or seemingly society at large, of the fact that a technologically-driven future will be disastrous if it is not guided by respect for human rights that is in turn grounded in law.

B. Ensuring legality and transparency

42. One of the most surprising characteristics of too many important digital welfare state initiatives is a lack of attention to the importance of ensuring legality. Many examples have been drawn to the Special Rapporteur's attention, including: the Australian Government's online compliance intervention system which used automated data-matching as the basis to send out vast numbers of debt notices with very high error rates (known as Robodebt);[83] allegedly unlawful information provided to claimants via the online Universal Credit portal in the United Kingdom;[84] the contested legality of the Irish Public Services Card for some of the purposes for which it has been used;[85] the SyRI (System Risk Indication) system in the Netherlands which initially lacked a legal basis and remains subject to court challenge;[86] and the Aadhaar system in India which was originally implemented without a legal framework.[87]

43. While the lack of a legal basis is deeply problematic per se, this gap also means that opportunities for legislative debate and for public inputs into shaping the relevant systems is also lacking. This has major potentially negative implications for transparency, design, legitimacy, and the likelihood of acceptance.

C. Promoting digital equality

44. Egalitarianism is a consistent theme of the technology industry, as exemplified by Facebook's aim "to give people the power to build community and bring the world closer together".[88] But at the macro

Social Research (2019) 449, at 473.

83 Terry Carney, 'The New Digital Future for Welfare: Debts Without Legal Proofs or Moral Authority?', *UNSW Law Journal Forum* (March 2018).

84 https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/ChildPovertyActions Group_1.pdf.

85 Final Investigation Report: 'An investigation by the Data Protection Commission in respect of the processing of personal data by the Department of Employment Affairs and Social Protection in relation to the Public Services Card ("PSC") examining compliance with the obligations in relation to Legal Basis and Transparency' (2019), at https://www.welfare.ie/en/pdf/pr170919.pdf.

86 Brief by the United Nations Special Rapporteur on extreme poverty and human rights as Amicus Curiae in the case of NJCM c.s./De Staat der Nederlanden (SyRI) before the District Court of The Hague (case number: C/09/550982/ HA ZA 18/388) (September 2019), at https://www.ohchr.org/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf.

87 Submission to the Special Rapporteur by National Law University Delhi, available from: https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/NationalLawUniversityDelhi.pdf.

88 Kevin Munger, 'The Rise and Fall of the Palo Alto Consensus', New York Times, 10 June 2019.

level Big Tech has been a driver of growing inequality[89] and has facilitated the creation of a 'vast digital underclass'.[90]

45. For its part, the digital welfare state sometimes gives beneficiaries the option to go digital or continue using more traditional techniques. But in reality, policies such as 'digital by default' or 'digital by choice' are usually transformed into 'digital only' in practice. This in turn exacerbates or creates major disparities among different groups. A lack of digital literacy leads to an inability to use basic digital tools at all, let alone effectively and efficiently. Limited access, or no access to the internet, poses huge problems for a great many people. Additional barriers arise for individuals who have to pay high prices to obtain internet access, to travel long distances or absent themselves from work to do so, visit public facilities such as libraries in order to get access, or obtain assistance from staff or friends to navigate the systems. And while the well-off might have instant access to up-to-date, and easy to use computers and other hardware, as well as fast and efficient broadband speeds, the least well off are far more likely to be severely disadvantaged by out of date equipment and time-consuming and unreliable digital connections.

46. Submissions to the Special Rapporteur from a wide range of countries emphasized the salience of these different problems. Both in the Global North and the Global South, many individuals, and especially those living in poverty, do not have a reliable internet connection at home, [91] cannot afford such a connection,[92] are not digitally skilled or confident,[93] or are otherwise inhibited in communicating with authorities online. The various submissions emphasize how these problems impede the ability of would-be claimants to realize their human rights.

47. The United Kingdom provides an example of a wealthy country in which, even in 2019, 11.9 million people (22% of the population) do not have the 'essential digital skills' needed for day-to-day life. An additional 19% cannot perform fundamental tasks such as turning on a device or opening an app. In addition, 4.1 million adults (8%) are offline because of fears that the internet is an insecure environment, and proportionately almost half of those are from a low income household and almost half are under sixty years of age.[94]

89 Isobel Asher Hamilton, 'A definitive list of the 13 richest tech billionaires in the world', *Business Insider*, 9 March 2019, available from: https://www.businessinsider.nl/net-worth-13-richest-tech-billionaires-in-the-world-2019-3?international=true&r=US.

90 Farhad Manjoo, 'The Tech Industry is Building a Vast Digital Underclass', *The New York Times*, 24 July 2019.

91 https://www.wired.com/story/global-internet-access-dire-reports/; https://data.oecd.org/ict/internet-access.htm; https://www.oecd.org/internet/oecd-toolkit-aims-to-spur-high-speed-internet-use-in-latin-america-and-the-caribbean.htm.

92 https://a4ai.org/affordability-report/report/2018/#2018:_where_are_we_on_the_road_to_affordable_universal_internet_access?; https://webfoundation.org/2019/03/new-mobile-broadband-pricing-data-reveals-stalling-progress-on-affordability/; In the United States, 27% of the population does not use high-speed broadband internet at home, and that figure is as high as 44% for people with an income below $30,000: https://www.pewinternet.org/fact-sheet/internet-broadband/.

93 European Commission, 'Human Capital: Digital Inclusion and Skills' (2019).

94 'The Digitally Disadvantaged', in *UK Consumer Digital Index 2019 – Key Findings* (Lloyds Bank 2019).

48. These problems are compounded by the fact that when digital technologies are introduced in welfare states, their distributive impact is often not a significant focus of governments.[95] In addition, vulnerable individuals are not commonly involved in the development of IT systems and the IT professionals are often ill-equipped to anticipate the sort of problems that are likely to arise.[96] Programs often assume, without justification, that individuals will have ready access to official documents and be able to upload them, that they will have a credit history or broader digital financial footprint, or even that their fingerprints will be readable, which is often not the case for those whose working lives have involved unremitting manual labour.

49. In terms of digital welfare policy, several conclusions emerge. First, there should always be a genuine non-digital option available.[97] Second, programs that aim to digitize welfare arrangements should be accompanied by programs designed to promote and teach the needed digital skills and to ensure reasonable access to the necessary equipment as well as effective online access. Third, in order to reduce the harm caused by incorrect assumptions and mistaken design choices, digital welfare systems should be co-designed by their intended users and evaluated in a participatory manner.

D. Protecting economic and social rights in the digital welfare state

50. The processes of digitization and the increasing role played by automated decision-making through the use of algorithms and artificial intelligence have, in at least some respects, facilitated a move towards a bureaucratic process and away from one premised on the right to social security or the right to social protection. Rather than the ideal of the State being accountable to the citizen to ensure that the latter is able to enjoy an adequate standard of living, the burden of accountability has in many ways been reversed. To a greater degree than has often been the case in the past, today's digital welfare state is often underpinned by the starting assumption that the individual is not a rights-holder but rather an applicant. In that capacity, a person must convince the decision-maker that they are 'deserving', that they satisfy the eligibility criteria, that they have fulfilled the often onerous obligations prescribed, and that they have no other means of subsistence. And much of this must be done electronically, regardless of the applicant's skills in that domain.

51. The right to social security[98] encompasses the right "to access and maintain benefits, whether in cash or in kind, without discrimination".[99] The imposition of technological requirements can make it impossible or

95 https://www.nytimes.com/2019/04/25/opinion/privacy-poverty.html.

96 Submission to the Special Rapporteur by ICTU, available from: https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/ITCU.pdf.

97 Association for Progressive Communications, Derechos Digitales and Media Matters for Democracy, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/APC_DrechosDigitalesMedia.pdf; Citizens Advice Scotland, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/CitizensAdviceScotland.pdf; National Social Security Rights Network, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/NationalSocialSecurityRightsNetwork.pdf.

98 Article 9 of the International Covenant on Economic, Social and Cultural Rights (ICESCR).

99 Committee on Economic, Social and Cultural Rights, The Right to Social Security, General Comment No. 19 (2007), para. 2.

very difficult for individuals to effectively access that right, thus making it effectively unaffordable.[100]

52. The right to social protection is integrally linked to what the Human Rights Committee refers to as the right to life with dignity, which must be protected, where necessary, through "measures designed to ensure access without delay by individuals to essential goods and services such as food, water, shelter, health-care, electricity and sanitation, and other measures designed to promote and facilitate adequate general conditions … ."[101] Various other rights are also implicated, including the right to an adequate standard of living, the right to mental health, and the right to be treated with dignity.

53. While social protection in general should be designed to protect these rights, the dignity dimension is at particular risk in the context of the digital welfare state. The potential risks arise in various contexts. First, the process for determining eligibility can easily be transformed into an electronic question and answer process that almost inevitably puts already vulnerable individuals at even greater disadvantage. Second, the way in which determinations are framed and communicated can be dehumanized and allow no room for meaningful questioning or clarification.

54. Third, the digital welfare state often seems to involve various forms of rigidity and the robotic application of rules. As a result, extenuating circumstances such as being late for an appointment because of urgent caring obligations, or being unable to understand a written communication whether because of a disability or a personal crisis, are often not taken into account in a predominantly digital context. Fourth, digital systems are often not designed to respond rapidly either to serious emergencies or to the daily challenges experienced by an older person whose entitlement has suddenly and inexplicably been electronically reduced or cancelled, or by a single parent unable to take a child to a local day care because the digital ID card will not function.

55. Fifth, the ways in which services are provided can easily have degrading connotations, such as unnecessarily exposing to a broader audience the fact that a person is reliant on benefits, or requiring extended waiting periods, or the navigation of lengthy queues. Sixth, the introduction of various new technologies that eliminate the human provider can enhance efficiency and provide other advantages, but might not necessarily be satisfactory for individuals who are in situations of particular vulnerability. New technologies often operate on the law of averages, in the interests of majorities, and on the basis of predicted outcomes or likelihoods.

56. Sixth, digital services risk eliminating, almost entirely, much of the human interaction and compassion that are likely to be indispensable components in providing at least some welfare recipients with the care and assistance they need. The assumption that there is always a technological fix for any problem is highly likely to be misplaced in various aspects of a humane and effective system of social protection.

[100] Id, paras. 24-27.

[101] Human Rights Committee, General Comment No. 36 (2018) on article 6 of the International Covenant on Civil and Political Rights, on the right to life, para. 26.

E. Protecting civil and political rights in the digital welfare state

57. That the poor suffer from more intense levels of scrutiny, monitoring, surveillance, is hardly an original observation. In the 1960s, Charles Reich wrote that welfare recipients in the United States "have been subjected to many forms of procedure and control not imposed on other citizens. … [They] are all too easily regulated."[102] In 1975, Michel Foucault wrote about the 'coercive technologies of behavior' used in modern society to 'discipline and punish' the poorer classes.[103]

58. By way of explaining why these lessons have not been learned in the digital welfare state, Shoshana Zuboff writes that the system of 'surveillance capitalism' that prevails today is unprecedented, which "has enabled it to elude systematic contest because it cannot be adequately grasped with our existing concepts."[104] This private surveillance is being reinforced by trends in government surveillance. Jack Balkin has described the 'National Surveillance State' as "a permanent feature of governance [that] will become as ubiquitous in time as the familiar devices of the regulatory and welfare states."[105]

59. Digital technologies are employed in the welfare state to surveil, target, harass and punish beneficiaries, especially the poorest and most vulnerable among them. Once again, many of the submissions received by the Special Rapporteur serve to illustrate and reinforce this point. They serve to highlight a number of human rights concerns. First, in the context of social security benefits and assistance, there is a real risk that beneficiaries are effectively forced to give up their right to privacy and data protection to receive their right to social security as well as other social rights.[106]

60. A second concern is the blurring of the lines between public and private surveillance. Welfare state authorities increasingly rely, either actively or passively, on private corporations for the surveillance and targeting of beneficiaries. Private entities have different motives for their involvement in benefit and social assistance systems and this may lead to conflicts between the public interests these systems ought to serve and the private interests of corporations and their owners.

61. A third concern is the potential for deliberate targeting and harassment of the poor through new technologies in the welfare state. As one submission to the Special Rapporteur highlights, fraud in the welfare state is often the result of confusion, complexity and the inability to correct the resulting errors.[107] But by deliberately using the power of new technologies to identify fraud or violations of 'conditionalities' imposed on beneficiaries, governments are likely to find inconsistencies that they can hold against claimants. It is relevant here that new technologies are enabling what Jack Balkin described as

[102] Charles A. Reich, 'Individual Rights and Social Welfare: The Emerging Legal Issues', *74 Yale L.J.* (1965), p. 1245.

[103] Michel Foucault, *Discipline and Punish: The Birth of the Prison* (1991), p. 222.

[104] Shoshana Zuboff, *The Age of Surveillance Capitalism* (2019), p. 14.

[105] Jack Balkin, 'The Constitution in the National Surveillance State', *Minnesota Law Review* (Vol. 93, 2008), p. 1-18.

[106] Submission to the Special Rapporteur by the Government of Mexico; Statement on Visit to the USA, by Professor Philip Alston, United Nations Special Rapporteur on extreme poverty and human rights, 15 December 2017, para 57.

[107] International Confederation of Trade Unions, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/ITCU.pdf.

the ‘death of amnesia’: new abilities to collect information and store it digitally for an undefined period of time create a future in which a wealth of information can be held against someone indefinitely.[108]

62. Additional concerns which warrant greater consideration than can be provided in the present report include (i) the human rights consequences of the move to predicting risk instead of the ex post enforcement of rules violations;[109] (ii) the dangers of connecting government data siloes which is more readily contemplated in the welfare context than elsewhere in the field of digital governance;[110] (iii) the psychological and societal cost of constant monitoring and surveillance;[111] and (iv) the growing tendency of some governments to use the opportunities provided by the digital welfare state to try to alter social behaviours whether in the form of sexual activity or preferences, approaches to cohabitation, the use of alcohol or drugs, the decision to have children, or many other such goals.[112]

F. Resisting the inevitability of a digital only future

63. Digital technologies in general, and especially those central to the digital welfare state, are often presented as being both unavoidable and irresistible. If a country wants to be seen to be at the technological cutting edge, if its government wants to have the most efficient, economical and flexible welfare system available, and if its citizenry wants all of the convenience that comes from not having to provide ID in order to undertake various transactions, then a transition to a digital welfare state must be pursued. But quite apart from the choices that citizens and governments might make if they were fully informed and adequately consulted, the reality is that such decisions are all too often taken in the absence of sophisticated cost-benefit analyses. And when such analyses are undertaken, they consist of financial balance sheets that ignore what might be termed the fiscally invisible intangibles that underpin human rights. Values such as dignity, choice, self-respect, autonomy, self-determination, privacy, and a range of other factors are all traded off without being factored into the overall equation, all but guaranteeing that insufficient steps will be taken to ensure their role in the new digital systems.

64. It is often assumed that at least some of these tradeoffs can be justified on the grounds that the bargain is just a matter between the individual and a particular government agency. But such an image is increasingly very far from the truth as cross-matching, data sharing, and cross-verification systematically enlarge the pools of data potentially available across the spectrum of government. To the extent

[108] Jack Balkin, ‘The Constitution in the National Surveillance State’, *Minnesota Law Review* (Vol. 93, 2008), p. 13.

[109] Id, p. 11.

[110] https://www.washingtonpost.com/news/theworldpost/wp/2018/08/09/aadhaar/?utm_term=.8a17992dfb6e.

[111] “In our research with civil society groups … concerns about stigmatisation and feelings of being targeted were more prominent than privacy concerns per se.” Data Justice Lab, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/UniversityCardiff.pdf.

[112] Cf Foucault’s analysis of Panoptic systems that could “be used as a machine to carry out experiments, to alter behaviour, to train and correct individuals”. Michel Foucault, *Discipline and Punish: The Birth of the Prison* (1991), p. 203.

that assurances are given that leakage from one silo to the next will not occur, such guarantees are largely illusory since a change of government or a real or imagined emergency situation is all that is required to trigger a partial or comprehensive breaking down of the partitions, quite apart from the risks of electronic data breaches due to hacking or normal system breakdowns. In addition, the assumption that the relationship is only that between government and citizen is also anachronistic. Corporate actors are now centrally involved in large parts of the welfare system, and when taken together with the ever-expanding reach of other forms of surveillance capitalism, intangible human rights values can be assumed to be worth as much as the shares of a bankrupt corporation.

65. The Special Rapporteur has learned of situations in which crucial decisions to go digital have been taken by government ministers without consultation, or even by departmental officials without any significant policy discussions taking place, on the grounds that the move is essentially an administrative matter, rather than involving a potentially game-changing approach to a large swathe of official policy. Sometimes there seems to be a presumption that even if the move to digital is not currently necessary, it surely will be one day and it is better to move in advance. Support for such pre-emptive moves may come from corporate interests, as well as from the security and counter-terrorism sectors, albeit for quite different reasons. Careful and transparent consideration should always be given to the questions of why, for whom, when, and how transitions to digital systems take place.

66. And even where detailed cost estimates are provided, this is an area in which accuracy seems difficult to achieve. Helen Margetts has observed that in the United Kingdom, for example, "[t]echnology and the public sector have rarely been happy bedfellows" and "every government technology project seems doomed to arrive late, underperform and come in over budget."[113] Another example is the Aadhaar system in India which is said to have lacked a proper cost-benefit analysis prior to implementation[114] and in relation to which there has been great disagreement as to the post hoc assessment of costs and benefits.[115]

G. The role of the private sector

67. Two consistent themes of this report have been the reluctance of many governments to regulate the activities of technology companies, and the strong resistance of those companies to taking any systematic account of human rights considerations. The fact that this leads to many large technology corporations operating in an almost human rights free-zone is further exacerbated by the extent to which the

[113] https://theconversation.com/back-to-the-bad-old-days-as-civil-service-infighting-threatens-uks-only-hope-for-digital-government-47683.

[114] National Law University Delhi, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/NationalLawUniversityDelhi.pdf.

[115] Reetika Khera, 'A 'Cost-benefit' Analysis of UID', *Economic and Political Weekly*, Vol. 48, No. 5 (2 February, 2013), p. 13-15; https://www.iisd.org/gsi/subsidy-watch-blog/estimating-impact-indias-aadhaar-scheme-lpg-subsidy-expenditure; https://economictimes.indiatimes.com/blogs/et-commentary/aadhaars-11-bn-question/; https://thewire.in/economy/the-curious-case-of-the-world-bank-and-aadhaar-savings; and https://qz.com/india/1519209/why-india-cant-cite-world-bank-to-brag-about-aadhaar/.

private sector is taking a leading role in designing, constructing, and even operating significant parts of the digital welfare state.[116]

68. Among well-known examples are the involvement of Net 1subsidiary Cash Paymaster Services (CPS), MasterCard and Grindrod Bank in the distribution of social grants linked to South Africa's biometric identification system, the roles played by Indue and Visa in the Cashless Debit Card trials in Australia, and IBM's involvement in Ontario's Social Assistance Management System. Submissions to the Special Rapporteur have also drawn attention to the increasing role of the private sector in the German market for public administration software used for unemployment services, social and youth welfare;[117] and outsourcing by United Kingdom local authorities to private companies in the area of social protection.[118] In contrast, various submissions point to the deliberate choice by governments involved *not* to rely on private actors to play key roles in the welfare state.[119]

69. The Special Rapporteur has addressed elsewhere the issues arising out of the privatization of public services more generally.[120] But in relation to social protection services there is a deeply problematic lack of information about the precise role and responsibility of private actors in proposing, developing and operating digital technologies in welfare states around the world. This lack of transparency has a range of causes, from gaps in freedom of information laws, confidentiality clauses, and intellectual property protections, through a failure on the part of legislatures and executives to require transparency, to a general lack of investigation of these practices by oversight bodies and the media.[121] The absence of information seriously impedes efforts to hold governments and private actors accountable.

H. Accountability mechanisms

70. Many of the programs used to promote the digital welfare state have been designed by the very same companies that are so deeply resistant to abiding by human rights standards. Moreover those companies and their affiliates are increasingly relied upon to design and implement key parts of the actual welfare programs. It is thus evident that the starting point for efforts to ensure human rights-compatible

116 Government of Ireland, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/Ireland.pdf ; Government of Estonia, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/Estonia.docx; Submission to the Special Rapporteur by the Government of Croatia.

117 AlgorithmWatch, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/AlgorithmWatch.pdf.

118 Data Justice Lab, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/UniversityCardiff.pdf.

119 University of Auckland, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/UniversityAuckland.docx; Submission to the Special Rapporteur by the Government of Greece; Submission to the Special Rapporteur by the Government of Argentina.

120 A/73/396 (2018).

121 AlgorithmWatch, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/AlgorithmWatch.pdf; Privacy International, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/PrivacyInternational.pdf; Irish Council for Civil Liberties, at https://www.ohchr.org/Documents/Issues/Poverty/DigitalTechnology/IrishCouncilCivilLiberties.pdf.

digital welfare states outcomes is to ensure through governmental regulation that technology companies are legally required to respect applicable international human rights standards.[122]

IV. Conclusions

71. **There is no shortage of analyses warning of the dangers for human rights of various manifestations of digital technology and especially artificial intelligence. But these studies focus overwhelmingly on the traditional civil and political rights such as the right to privacy, non-discrimination, fair trial rights, and the right to freedom of expression and information. With a handful of exceptions, none has adequately captured the full array of threats represented by the emergence of the digital welfare state. The vast majority of states spend very large amounts of money on different forms of social protection, or welfare, and the allure of digital systems that offer major cost savings along with personnel reductions, greater efficiency, and fraud reduction, not to mention the kudos associated with being at the technological cutting edge, is irresistible. There is little doubt that the future of welfare will be integrally linked to digitization and the application of AI.**

72. **But as humankind moves, perhaps inexorably, towards the digital welfare future it needs to alter course significantly and rapidly to avoid stumbling zombie-like into a digital welfare dystopia. Such a future would be one in which: unrestricted data matching is used to expose and punish the slightest irregularities in the record of welfare beneficiaries (while assiduously avoiding such measures in relation to the well-off); evermore refined surveillance options enable around the clock monitoring of beneficiaries; conditions are imposed on recipients that undermine individual autonomy and choice in relation to sexual and reproductive choices, and in relation to food, alcohol and drugs and much else; and highly punitive sanctions are able to be imposed on those who step out of line.**

73. **It will reasonably be objected that this report is unbalanced, or one-sided, because the dominant focus is on the risks rather than on the many advantages potentially flowing from the digital welfare state. The justification is simple. There are a great many cheerleaders extolling the benefits, but all too few counselling sober reflection on the downsides. Rather than seeking to summarize the analysis above, a number of additional observations are in order.**

74. **First, digital welfare state technologies are not the inevitable result of 'scientific' progress, but instead reflect political choices made by humans. Assuming that technology reflects pre-ordained or objectively rational and efficient outcomes risks abandoning human rights principles along with democratic decision-making.**

[122] See Yeung et al, above; Paul Nemitz, 'Constitutional Democracy and Technology in the Age of Artificial Intelligence', *Philosophical Transactions, A* 376 (2018); and Karen Yeung, 'A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework', Council of Europe doc. MSI-AUT(2018)05 rev (22 May 2019).

75. **Second, if the logic of the market is consistently permitted to prevail it inevitably disregards human rights considerations and imposes "externalities on society, for example when AI systems engage in bias and discrimination … and increasingly reduce human autonomy".**[123]

76. **Third, the values underpinning and shaping the new technologies are unavoidably skewed by the fact that there is "a diversity crisis in the AI sector across gender and race".**[124] **Those designing AI systems in general, as well as those focused on the welfare state are overwhelmingly white, male, well-off, and from the Global North. No matter how committed they might be to certain values, the assumptions and choices made in shaping the digital welfare state will reflect certain perspectives and life experiences. The way to counteract these biases and to ensure that human rights considerations are adequately taken into account is to ensure that the "practices underlying the creation, auditing, and maintenance of data" are subjected to very careful scrutiny.**[125]

77. **Fourth, predictive analytics, algorithms and other forms of AI are highly likely to reproduce and exacerbate biases reflected in existing data and policies. In-built forms of discrimination can fatally undermine the right to social protection for key groups and individuals. There therefore needs to be a concerted effort to identify and counteract such biases in designing the digital welfare state. This in turn requires transparency, and broad-based inputs into policy-making processes. The public, and especially those directly affected by the welfare system, need to be able to understand and evaluate the policies that are buried deep within the algorithms.**

78. **Fifth, especially but not only in the Global North, the technology industry is heavily oriented towards designing and selling gadgets for the well-off such as driverless and flying cars and electronic personal assistants for multi-tasking businessmen [sic]. In the absence of fiscal incentives, government regulation, and political pressures, it will devote all too little attention to facilitating the creation of a welfare state that takes full account of the humanity and concerns of the less well-off in any society.**

79. **Sixth, to date astonishingly little attention has been paid to the ways in which new technologies might transform the welfare state for the better. Instead of obsessing about fraud, cost savings, sanctions, and market-driven definitions of efficiency, the starting point should be on how existing or even expanded welfare budgets could be transformed through technology to ensure a higher standard of living for the vulnerable and disadvantaged, to devise new ways of caring for those who have been left behind, and more effective techniques for addressing**

123 Anton Korinek, 'Integrating Ethical Values and Economic Value to Steer Progress in Artificial Intelligence' (2019) p. 2, at http://www.nber.org/papers/w26130.

124 Sarah West, Meredith Whittaker, and Kate Crawford, *Discriminating Systems: Gender, Race and Power in AI* (AI Now Institute, 2019) (Women make up "15% of AI research staff at Facebook and 10% at Google. … [and] only 2.5% of Google's workforce is black, while Facebook and Microsoft are each at 4%.").

125 Rashida Richardson, Jason M. Schultz, and Kate Crawford, 'Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice', 94 *New York University Law Review* (2019) 192, at 225.

the needs of those who are struggling to enter or re-enter the labour market. That would be the real digital welfare state revolution.